(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－256144
（P2003－256144A）
(43)公開日　平成15年９月10日(2003.9.10)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	3/06	３０１	Ｇ０６Ｆ	3/06	３０１Ｍ　５Ｂ０６５
		３０４			３０４Ｈ　５Ｂ０８２
	12/00	５４５		12/00	５４５Ａ　５Ｂ０８９
	13/00	３５１		13/00	３５１Ｂ

審査請求　未請求　請求項の数10　ＯＬ　（全 19 頁）

(21)出願番号　特願2002－52620(P2002－52620)

(22)出願日　平成14年２月28日(2002.2.28)

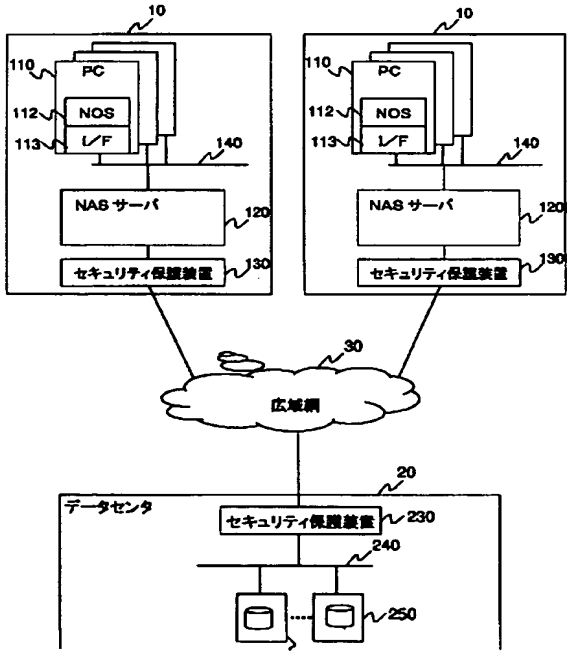
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　加納　義樹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　北村　学
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　記憶装置

(57)【要約】
【課題】ユーザがデータの保管場所を意識することなく安全にファイルにアクセスできる手段を提供する。
【解決手段】１または複数台の計算機１１０とＬＡＮ１４０を介して接続され、これら計算機からファイルデータのアクセス要求を受け付けるサーバ装置１２０と、サーバ装置１２０と広域網３０を介して接続され、ファイルデータを記憶する記憶装置２５０が設けられる。計算機１１０とサーバ装置１２０との間の通信は、ネットワークファイルプロトコルを用いて行われ、サーバ装置と記憶装置との間の通信は、ブロックデバイスプロトコルを用いて行われる。サーバ装置１２０及び記憶装置２５０は、それぞれ、セキュリティ装置１３０、２３０を介して広域網に接続される。

図1



【特許請求の範囲】
【請求項１】記憶装置と、
前記記憶装置に格納されるファイルデータの格納場所、及びアクセス状態を管理する管理情報を保持する管理サーバと、
ネットワークを介して計算機より第１のプロトコルでファイルデータのアクセス要求を受け付け、前記管理情報に基づいて前記計算機からアクセス要求に応じ、第２のプロトコルで前記記憶装置へのアクセスを行うサーバ装置とを有することを特徴とする記憶装置システム。
【請求項２】前記第１のプロトコルは、ネットワークファイルアクセスプロトコルであって、前記第２のプロトコルはブロックデバイスプロトコルであることを特徴とする請求項１記載の記憶装置システム。
【請求項３】前記ブロックデバイスプロトコルとしてｉＳＣＳＩを用いたことを特徴とする請求項２記載の記憶装置システム。
【請求項４】前記サーバ装置と、前記記憶装置とは、セキュリティ保護装置を介して接続されることを特徴とする請求項２記載の記憶装置システム。
【請求項５】データを記憶する第１の記憶装置と、
データを記憶する第２の記憶装置と、
前記第１の記憶装置とローカルに接続され、前記第２の記憶装置と広域網を介して接続されるサーバ装置であって、ローカルなネットワークを介して計算機よりファイルデータのアクセス要求を受け付け、該アクセス要求によりアクセスすべきデータが前記第１及び第２の記憶装置のいずれに格納されているかを判別し、該判別の結果に応じて前記第１の記憶装置、または前記第２の記憶装置へのアクセスを行うサーバ装置とを有する記憶装置システム。
【請求項６】前記サーバ装置とネットワークを介して接続され、前記第２の記憶装置に格納されるデータの格納位置、及びアクセス状態を管理するための情報を保持する管理サーバを有することを特徴とする請求項５記載の記憶装置システム。
【請求項７】前記サーバ装置は、前記第２の記憶装置に格納されたデータをアクセスする際、前記管理サーバにアクセス要求を発行し、該アクセス要求に対する応答に基づいて前記第２の記憶装置をアクセスすることを特徴とする請求項６記載の記憶装置システム。
【請求項８】前記サーバ装置は、セキュリティ保護装置を介して前記第２の記憶装置と接続されることを特徴とする請求項５記載の記憶装置システム。
【請求項９】前記サーバ装置を複数備え、前記第２の記憶装置には、該複数のサーバ装置により共用されるデータが格納されることを特徴とする請求項６記載の記憶装置システム。
【請求項１０】データを記憶する記憶装置と、
前記記憶装置と広域網を介して接続されるサーバ装置であって、ローカルなネットワークを介して計算機よりネットワークファイルプロトコルを用いたファイルデータへのアクセス要求を受け付け、該アクセス要求に応答して、前記記憶装置に格納されたファイルデータをブロックデバイスプロトコルを用いてアクセスするサーバ装置とを有することを特徴とする記憶装置システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、計算機により利用されるデータを管理する記憶装置システムに係り、特に、広域網を介してデータを管理することの可能な記憶装置システムとそのファイルの保管、管理方法に関する。
【０００２】
【従来の技術】近年、情報化の進展により、企業等で作成されるデータは、飛躍的に増えてきている。例えば、企業内においては、各部署でデータが作成されるため、必然的にデータの管理も各部署で行われている。企業におけるデータ管理の一例として、作成されたデータのバックアップがある。バックアップでは、例えば、磁気ディスク装置に格納されている業務上重要な情報（データ）が、磁気ディスク装置からテープデバイス等の二次記憶装置にコピーされる。バックアップの頻度も、データの増大に伴い増大している。
【０００３】このようなデータの管理を集約的に管理することにより、データの管理を一元的に行うことができ、企業でのデータ管理に要するコストの削減が可能になる。例えば、データが各部署に分散されており、各部署で日々バックアップを行うより、情報を集約化し、一元化して管理を行う方が効率的であって望ましい。
【０００４】情報の一元化に適した装置として、ＲＡＩＤに代表されるような高信頼な大容量記憶装置がある。ＲＡＩＤでは、数テラバイトの記憶領域を複数の小さな論理的な記憶領域に分けることで、集約的に小さなグループごとの情報を１つにまとめることができる。このようなＲＡＩＤの特徴を生かして、企業内の各部署で分散して管理されていたデータが、情報部門内の大型計算機センタ等において、一元的に管理されるようになってきた。
【０００５】このようなデータの一元管理の流れは、企業内にとどまらない。最近では、データセンタにおいて、複数の企業のデータを受託管理するサービス業者が現れ始めている。データセンタでは、複数の企業のデータを安全にかつ迅速に管理することが求められており、情報をより容易に管理する手段が必要とされている。しかし、ＲＡＩＤでは、記憶領域をブロック単位としてデータが取り扱われるため、データセンタの管理者にとってその管理が難しい。
【０００６】一方で、ブロック単位での管理の難しさを

て、Network Attached Storage（略してＮＡＳ）と呼ばれるファイルサーバがある。ＮＡＳでは、パーソナルコンピュータ（ＰＣ）やワークステーションが備えるＮＦＳ（Network File System）やＣＩＦＳ(Common Internet File system)等のネットワークファイルプロトコルを用いたアクセスが可能である。このため、データ管理をファイル単位で行うことができ、ブロック単位での管理と比べてデータの管理が容易である。

【０００７】

【発明が解決しようとする課題】ＮＡＳで取り扱われるネットワークファイルプロトコルは、ローカルエリアネットワーク（ＬＡＮ）を前提にして作られている。このため、ネットワークとして広域網を適用すると、距離によるアクセスの遅延のためファイルへの安定したアクセスが行えず、結果としてデータの破壊を招く可能性がある。したがって、企業がＮＡＳを導入した場合、記憶装置の管理をデータセンタなどの外部に委託することが難しくなる。さらに、企業やデータセンタ等は、広域網からの不正進入を防ぐために、ファイアウォールなどのセキュリティ保護装置を多段に備えつけることが多いため、データセンタでＮＡＳを管理したとしても、企業のＰＣからデータセンタ内のＮＡＳへ接続することは非常に難しい。

【０００８】本発明の目的は、広域網を介して接続されるＮＡＳサーバとデータセンタ間で、安全な論理通信網を構築し、データセンタ内の記憶装置をＮＡＳサーバで利用を可能にして、データセンタ内で保管されたデータを複数のＮＡＳサーバ間で共有する手段を提供することにある。

【０００９】

【課題を解決するための手段】本発明によれば、１または複数台の計算機とＬＡＮを介して接続され、これら計算機からファイルデータのアクセス要求を受け付けるサーバ装置と、該サーバ装置と広域網を介して接続され、前記ファイルデータを記憶する記憶装置とを有する。サーバ装置は、計算機からのアクセス要求に応じて、記憶装置に保持されたファイルデータをアクセスする。

【００１０】本発明の好ましい態様において、計算機とサーバ装置との間の通信は、ネットワークファイルプロトコルを用いて行われ、サーバ装置と記憶装置との間の通信は、ブロックデバイスプロトコルを用いて行われる。サーバ装置及び記憶装置は、それぞれ、セキュリティ装置を介して広域網に接続される。

【００１１】本発明の一つの態様において、サーバ装置は、自身に直接接続される内部記憶装置を備える。サーバ装置は、外部の記憶装置及び内部の記憶装置に記憶されるファイルデータの管理情報を保持し、計算機からのアクセス要求に応じて、アクセスすべきファイルデータの格納位置を判別し、外部記憶装置、あるいは内部記憶装置をアクセスする。

【００１２】本発明の他の態様においては、複数のサーバ装置と広域網を介して接続されるサーバ管理装置が設けられる。サーバ管理装置は、複数のサーバ装置により共有される記憶装置を管理するための管理情報を保持し、サーバ装置間での記憶装置の共有状態を管理する。

【００１３】管理情報は、記憶装置の共有に先立って管理者により設定される。各サーバ装置は、計算機から他のサーバ装置との間で共有している記憶装置へのアクセス要求を受けると、サーバ管理装置にアクセス許可を求める。サーバ管理装置では、この要求に応答して、要求元のサーバ装置が記憶装置の共有を許可されているか調べ、許可されている場合に、アクセスを許可し、アクセスされるべきファイルデータの記憶位置をサーバ装置に通知する。サーバ装置は、受け取った記憶位置に基づいて対象とされるべきファイルデータをアクセスする。

【００１４】

【発明の実施の形態】図１は、本発明が適用された計算機システムの一実施形態における構成を示す簡略なブロック図である。

【００１５】本実施形態における計算機システムは、企業内に設けられる計算機システム１０と、１又は複数の企業内計算機システム１０により利用されるデータの管理を行うデータセンタ２０を構成する計算機システムが、広域網３０を介して相互に接続された構成を有する。ここで、広域網３０とは、インターネットのようなＩＰ網、ＡＴＭ（Asynchronous Transfer mode）網、公衆網など、複数の利用者が通信路を共有することのできるネットワークをいう。また、一般には、企業内計算機システム１０とデータセンタ２０とは、物理的、あるいは地理的に離れた場所に設けられる。

【００１６】企業内計算機システム１０は、複数台のパーソナルコンピュータ（ＰＣ）１１０、ＮＡＳサーバ１２０、セキュリティ保護装置１３０、ＰＣ１１０、ＮＡＳサーバ１２０を相互に接続するローカルエリアネットワーク（ＬＡＮ）１４０を有しており、セキュリティ保護装置１３０により広域網３０と接続されている。

【００１７】各ＰＣ１１０は、ネットワーク接続のためのインタフェース１１２と、ＣＩＦＳプロトコルやＮＦＳプロトコルに対応し、ネットワークファイルシステムを利用できるネットワークオペレーティングシステム（ＮＯＳ）１１３とを備える。ＰＣ１１０は、その他、ＣＰＵやメモリ、入出力装置などを有するが、これらについては、本発明と直接関係するものではなく、図示を省略する。ＰＣ１１０上で実行されるＮＯＳ１１３その他のプログラムは、ＰＣ１１０が有する記憶装置に格納される他、ＮＡＳサーバ１２０により提供される記憶領域に格納され、その実行時にＰＣ１１０のメモリにロードされるように構成されていてもよい。

【００１８】ＮＡＳサーバ１２０は、ＰＣ１１０に対して、それが利用する記憶領域を提供する。ＰＣ１１０

は、ＮＦＳやＣＩＦＳなどのネットワークファイルシステムを用いＮＡＳサーバ１２０の記憶領域を利用することができる。この記憶領域は、磁気ディスク装置で構成される。

【００１９】ＬＡＮ１４０と広域網３０との間の接続には、幾つかの形態が考えられる。本実施形態では、ＬＡＮ１４０と広域網３０との接続を、セキュリティ保護装置を介して行っている。セキュリティ保護装置１３０、２３０は、広域網３０からの不意なアクセスによるシステムへの侵入、破壊を防ぎ、計算機システム１０とデータセンタ２０との間で転送されるデータの盗聴、改ざんや、なりすましを防いだ通信を可能にする。具体的に、セキュリティ保護装置１３０は、広域網３０からの不特定なアクセスを禁止するために、TCP/IPにおける各サービスへの通信路を示すポートのうち、セキュリティ保護装置１３０、２３０間で利用されるポート以外のポートを閉塞し、セキュリティ保護装置間１３０、２３０で利用されるポートを用いて暗号化された通信路が用意される。暗号化は、各セキュリティ保護装置で予め設定された暗号鍵、暗号鍵の寿命、認証アルゴリズム、暗号アルゴリズム、及び、相手側セキュリティ保護装置のＩＰアドレスもしくはホスト名等を含む認証情報を用いて行われる。通信路の暗号化を行うプロトコルの一例としてはIPSecがあり、LANからWANへ接続する装置に備えつけられている。

【００２０】計算機システム１０のＬＡＮ１４０からデータセンタ２０のＬＡＮ２４０へのアクセスが、このように暗号化された通信路（以降、暗号化通信路という）を用いて実施される。また、その逆に、ＬＡＮ２４０から広域網３０経由でＬＡＮ１４０へアクセスする際にも、セキュリティ保護装置１３０、２３０間で作られる暗号化回線が用いられる。

【００２１】本実施の形態では、セキュリティ保護装置１３０がＮＡＳサーバ１２０に直接接続されているが、ＮＡＳサーバ１２０がセキュリティ保護装置１３０を通じて外部と通信するよう構成されていれば、ＬＡＮ１４０にセキュリティ保護装置１３０が接続されていてもよい。

【００２２】データセンタ２０は、広域網３０に接続するセキュリティ保護装置２３０、ＮＡＳサーバ１２０の記憶領域となる１又は複数台の記憶装置２５０を有する。セキュリティ保護装置２３０、及び記憶装置２５０は、相互にＬＡＮ２４０を介して接続される。

【００２３】記憶装置２５０は、データを保管するディスク装置とその制御を行う制御装置を含んで構成され、記憶領域となる論理的な記憶装置であるロジカルユニット（ＬＵ）を提供している。ＬＵをＮＡＳサーバ１２０等の装置へ提供するために、記憶装置２５０は、ＬＡＮ２４０を介してネットワーク上にＳＣＳＩプロトコルを

【００２４】図2は、ＮＡＳサーバ１２０の構成を示す機能ブロック図である。ＮＡＳサーバ１２０は、プロセッサ２２０、ネットワークインタフェース２１１、２１２及び記憶装置２１５を含んで構成される。

【００２５】ＮＡＳサーバ１２０は、ネットワークインタフェース２１１によりＬＡＮ１４０に、また、ネットワークインタフェース２１２によりセキュリティ保護装置１３０に接続される。プロセッサ２２０は、ネットワークインタフェース２１１、２１２を介して行われる通信で取得するデータの発信元を把握し、ファイルへのオペレーション情報を確認して記憶領域への処理を行う。

【００２６】プロセッサ２２０は、ネットワークプロトコル処理部２２１、ネットワークファイルシステム処理部（ネットワークＦＳ処理部）２２２、ファイルシステム管理部（ＦＳ管理部）２２３、ブロックデバイスプロトコル処理部２２４、記憶領域管理部２２５、セキュリティ部２２７、設定制御部２２８、及び設定部２２９を有する。プロセッサ２２０の有する各部の機能は、プロセッサ２２０上でのプログラム処理により実現される。

【００２７】ネットワークプロトコル処理部２２１は、ＴＣＰ／ＩＰのプロトコルに従った処理を行い、ネットワークインタフェース２１１、あるいは、２１２より取得されたデータから発信元を確認し、送信データを保証した通信を行う。

【００２８】ネットワークＦＳ処理部２２２は、ＰＣ１０よりＬＡＮ１４０経由で転送されるファイルオペレーションを処理し、ＦＳ管理部２２３で管理されるファイルシステムへの操作を行う。ファイルオペレーションの処理では、後述するエキスポート管理表の許可済みのディレクトリに対してのみ、ファイルシステムへの実際の操作を行う。未許可ディレクトリに関してはエラーを戻す。

【００２９】ファイルオペレーションは、与えられたディレクトリとファイル情報からファイルの有無を検索する“lookup”、検索したファイルへバイト単位での読み出し操作をする“Read”、そして、同様にファイルへバイト単位で書き出し操作をする“Write”等のオペレーションを含む。このようなファイル操作を行うネットワーク処理部の例として、ＮＦＳサーバやＣＩＦＳサーバがある。

【００３０】ＦＳ管理部２２３は、記憶装置２１５や記憶装置２５０から提供されるＬＵに記録されたファイルシステムの構造を示すスーパーブロック、ファイルを構成するi-node、そして、データとファイルシステム内のディレクトリ情報を記録するブロックに基づいて、ファイルシステムの構成を管理する。スーパーブロックは、ファイルシステムの構造を示すために、ファイルシステム内のi-node数、ブロック数、ブロックの利用可能開始領域の論理ブロックアドレス（ＬＢＡ）、ファイルシス

む。

【００３１】i-nodeは、ファイルシステム中で順序づけて保存されている。i-nodeには、ファイルの保護アクセス権を設定するモード、ファイルの所有者、ファイルサイズ、ファイルへの最終更新時刻、ファイルへのリンク数、アクセス可能なグループ、そして、データが含まれるブロックへのリンクに関する情報が含まれている。ファイルの場合にはブロックの１つにファイル名が記される。ディレクトリの場合には、そのディレクトリの中に存在するすべてのファイル名もしくはディレクトリ名と、その名前に対応するi-node番号と一対一に対応する情報が記憶装置内の論理ブロックに保管される。

【００３２】ＦＳ管理部２２３は、後述するファイルシステム管理表に基づいて、ＬＵ毎のファイルシステムを指定されたＮＡＳサーバ１２０内のファイルシステムへ複数個をマウントすることが可能である。ＦＳ管理部２２３は、ファイルシステムをマウントする際に、メモリ上にマウント済みリストとして、マウントした場所、ＬＵ、ファイルシステム管理の場所を示すディスク識別子を記録する。ファイルシステム管理の場所とは、ファイルシステムのスーパーブロック、i-node、ブロック情報の保管を行うＮＡＳサーバ１２０内のメモリ領域である。本実施形態では、メタデータ管理部２２３１がこの管理を行う。なお、ファイルの情報のi-nodeやブロック情報はアクセスの高速化のために、ＮＡＳサーバ内のメモリにキャッシュされてもよい。

【００３３】さらに、ＦＳ管理部２２３は、ネットワーク処理部２２２から命令されるファイルオペレーションを実行する。このファイルオペレーションは、“Lookup”を行うためのファイルの検索処理、検索されたファイルの操作を一意に決定する識別子を設定するためのファイルオープン処理、識別子からファイルへの実際のアクセスを行うための読み出し処理、書き出し処理を含む。このファイルオペレーションに、i-node内の情報を変更する処理を有しても良い。ＦＳ管理部２２３では、このi-nodeを用いてファイルのアクセス制御を行うメタデータ管理部２２３１を含み、複数のＰＣ１１０から同時に１つのファイルへアクセスする際にデータの一貫性保証を行っている。

【００３４】ブロックデバイスプロトコル処理部２２４は、ＦＳ管理部２２３より命令された記憶領域へのオペレーションの処理をＳＣＳＩのプロトコルに従って行う。ＦＳ管理部２２３から命令される処理は、２つに分けられる。第１は、i-nodeの情報への読み出しと書き出し命令、第２は、ブロックの情報への読み出しと書き出し命令である。読み出し命令はSCSIプロトコルのReadに対応し、書き出し命令はWriteに対応する。本実施形態では、i-nodeの情報は、より迅速なファイルの検索と更新を実施するために、ＮＡＳサーバ１２０内の記憶装置２１５に保持される。一方、ブロックの情報は、リモート側の記憶装置２５０に保持される。

【００３５】記憶領域管理部２２５は、記憶装置となる装置を検出、管理し、デバイスブロックプロトコル処理部２２４で発行された命令を、命令先のＬＵに対して実行する。記憶装置の検出は、ローカルの記憶装置２１５に関しては、ＳＣＳＩのＬＵの検出方法を用いて行われる。また、データセンタ２０にある記憶装置２５０の検出は、ＮＡＳサーバ１２０とデータセンタ２０内のＬＡＮ２４０との間で通信路が確立したあと、iSCSIのプロトコルに従って、記憶装置へのＩＰアドレスと記憶装置上のＬＵへのiSCSI名を用いて行われる。検出され記憶装置は、ローカルもしくはデータセンタ毎のＬＵとして利用される。記憶領域管理部２２５は、デバイスブロックプロトコル処理部２２４で発行された命令に応じて、管理しているローカルもしくはデータセンタのＬＵを指定したＳＣＳＩの命令を実行する。

【００３６】設定制御部２２６は、ネットワークプロトコル処理部２２１、ネットワークＦＳ処理部２２２、ＦＳ管理部２２３、そして記憶領域管理部２２５を統合的に管理する。

【００３７】設定部２２９は、設定制御部２２６に対する設定時のパラメータを入力する。

【００３８】設定制御部２２６は、他の各部の設定に関する情報を記録するため、ディスク管理表、接続パス管理表、セキュリティ保護装置管理表、ファイルシステム管理表、エキスポート管理表、及びファイルアクセス管理表を持つ。

【００３９】ディスク管理表は、ブロックプロトコル処理部２２４で利用され、記憶装置２５０から広域網３０を通じて提供されるＬＵごとに、そのユニークな名前であるディスク識別子、ＬＵのネットワーク上での所在を示すＩＰアドレス、ＬＵへの接続後にアクセスする記憶装置のiSCSI名などの情報を保持する。

【００４０】接続パス管理表は、記憶領域管理部２２５で利用され、記憶装置２５０等のＩＰアドレス、そして、計算機システム１０からデータセンタまでの経路上に設けられるセキュリティ保護装置のＩＰアドレスもしくはホスト名が登録される。本実施形態では、計算機システム１０のセキュリティ保護装置１４０からデータセンタ２０へアクセスする際、セキュリティ保護装置の数は１つであるが、複数のセキュリティ保護装置が存在した場合、セキュリティ保護装置の数のＩＰアドレスもしくはホスト名を有する。

【００４１】セキュリティ保護装置管理表は、各セキュリティ保護装置のＩＰアドレスまたはホスト名に対応して、そのセキュリティ保護装置での認証処理に用いられる認証情報が登録される。

【００４２】ファイルシステム管理表は、ＦＳ管理部２２３で利用され、ＮＡＳサーバ１２０でマウントするファイルシステムの情報が含まれる。その情報には、ファ

イルシステムを保管するＬＵのディスク識別子と、このディスク識別子で示されるＬＵのファイルシステムをマウントする場所が記述されている。例えば、ディスク識別子が“/dev/sd0a”、マウントする場所が“/mnt”だとすると、ＮＡＳサーバ１２０内には“/”としてルートファイルシステムが存在するので“mnt”というディレクトリの上に“/dev/sd0a”の中に含まれるファイルシステムがマウントされる。また、ファイルシステム管理表には、ＮＡＳサーバ１２０でのファイルシステムの管理方式、例えば、ファイルシステムのフォーマット、リードオンリもしくはリードとライトでファイルシステムをマウント、ファイルシステムのリカバリ方法等の情報を記述してもよい。これらについては、本実施形態の説明と直接には関係しないので説明を省略する。

【００４３】エキスポート管理表は、ネットワークＦＳ処理部２２２で利用され、複数のＰＣ１１０からのファイルオペレーションの操作をＮＡＳサーバ１２０で実施することが許可されるディレクトリを示す。これをエキスポートと呼ぶ。また、特定のＰＣ１１０に対するディレクトリ内のファイルオペレーションの許可もしくは不許可の管理を行うために、操作許可ホスト、操作不許可ホストを示す情報を含めてもよい。

【００４４】ファイルアクセス管理表は、ＮＡＳサーバ１２０のメモリ上に設けられ、ファイルのアクセス状態を管理するための情報が保持される。具体的に、ファイルアクセス管理表は、メタデータ管理部２２３１において、ネットワークＦＳ処理部２２２で行われる複数のＰＣ１１０からのファイルオペレーションを管理するために使われる。

【００４５】ファイルオペレーションの管理を行うために、ファイルアクセス管理表は、各ファイルのファイル名とそのファイル識別子、及び、ファイル識別子ごとに、i-node番号、並びにファイルを参照しているＰＣ１１０を示す情報を保持したアクティブ項目を有する。また、ファイルアクセス管理表は、一度アクセスしたファイルの履歴を管理し、I－nodeのキャッシュを行うときに利用している。

【００４６】ブロックデバイスプロトコル処理部２２５は、ＳＣＳＩ等、ブロック単位で記憶装置へのアクセスが可能なプロトコルを使用する。ここでは、内部の記憶装置２１５に対してはＳＣＳＩを使用し、広域網３０経由でアクセスする記憶装置２５０に対してはＴＣＰ／ＩＰを通信路として使用するｉＳＣＳＩを使用する。

【００４７】ネットワークインタフェース２１１、２１２は、ＬＡＮあるいは広域網上に形成されるＴＣＰ／ＩＰの通信路を用い、信頼性を保証したデータの転送を行うためのインタフェースである。

【００４８】記憶装置２１５は、ＮＡＳサーバでファイルシステムを構築し、ＰＣ１１０からのＬＡＮ経由でのファイルアクセスを提供する。本実施形態では、記憶装置２１５を磁気ディスク装置として説明するが、記憶装置として、フラッシュＲＯＭのような半導体素子を記憶媒体として用いたソリッドディスク装置や、複数のディスク装置により構成されるＲＡＩＤ装置を用いてもかまわない図４は、記憶装置２５０の構成を示す簡略化された機能ブロック図である。記憶装置２５０は、データを格納する磁気ディスク装置４２０と、磁気ディスク装置４２０へのアクセスの制御を行う記憶制御装置４１０を有する。記憶制御装置４１０は、ＬＡＮ２４０に接続するネットワークインタフェース４１５、ネットワークプロトコル処理部４１４、ブロックデバイスプロトコル処理部４１３、ファイバチャネル（ＦＣ）、ＳＣＳＩ等を介して、ディスク装置４２０に接続するチャネルインタフェース（チャネルＩ／Ｆ）４１１を有する。

【００４９】ネットワークプロトコル処理部４１４は、ＬＡＮ２４０を介して送られてくるメッセージをＬＡＮ２４０上でのＴＣＰ／ＩＰなどのプロトコルに従って処理し、アクセス要求を解釈する。また、磁気ディスク装置４２０から読み出されたデータをＬＡＮ２４０上のプロトコルに従ったメッセージとしてＬＡＮ２４０に送信する。

【００５０】ブロックデバイスプロトコル処理部４１３は、ＬＡＮ２４０を介して送られてきたアクセス要求からディスク装置４２０への操作を抽出し、チャネルインタフェース４１１を介し、磁気ディスク装置４２０のデータをアクセスする。

【００５１】記憶装置２５０は、単体の磁気ディスク装置４２０を用いた記憶装置の他、複数の磁気ディスク装置を用いたディスクアレイなどの記憶装置でもよい。記憶制御装置４１０は、１台の磁気ディスク装置４２０の記憶領域を複数の領域に分割し、分割された記憶領域をＬＵとして、あるいは、複数の磁気ディスク装置４２０に跨る記憶領域を１つのＬＵとして提供することができる。このような記憶領域の管理については、技術的に公知のものを適用することができるので、ここでは説明を省略する。

【００５２】本実施形態では、記憶媒体に磁気ディスクを適用した記憶装置を用いているが、例えば、光ディスクなど他の記憶媒体を用いた記憶装置であってもかまわない。さらに、記憶制御装置４１０は、図には示されていないが、磁気ディスク装置４２０に格納されるデータのコピーを一時的に保持するキャッシュを備えることができる。

【００５３】図５は、セキュリティ保護装置の構成を示す機能ブロック図である。ここでは、セキュリティ保護装置１３０を例に説明するが、セキュリティ保護装置２３０も同様に構成される。

【００５４】セキュリティ保護装置１３０は、プロセッサ５１０、ネットワーク（広域網３０、ＮＡＳサーバ１２０との通信路）に接続するためのネットワークインタ

フェース５２０、及び、後述する内部認証部５０６、外部認証部５０８での認証処理に使用される認証情報を格納した認証情報データベース（認証情報ＤＢ）５３０を格納した記憶装置とを有する。

【００５５】プロセッサ５１０は、ＴＣＰ／ＩＰのプロトコルに従ってメッセージ処理を行うネットワークプロトコル処理部５０５、内部ネットワークから広域網３０を介して外部のネットワークへ接続する際に認証処理を行う内部認証部５０６、内部認証部５０６での認証の後、外部のネットワークに暗号化された通信路の設定を要求するパス接続部５０７、外部から内部ネットワークへの接続に対する認証処理を行う外部認証部５０９、外部処理認証部５０９で認証された通信に対して暗号化された通信を確立するパス確立部５０８、及び、ネットワーク経由で認証情報の登録、管理を行う認証情報管理部５０１を有する。これら各部の機能は、プロセッサ５１０上でのプログラム処理により実現される。

【００５６】認証情報ＤＢ５０２には、認証情報として、接続相手側のセキュリティ保護装置と暗号化を行うための暗号鍵、暗号鍵の寿命、認証アルゴリズム、暗号アルゴリズム、及び相手側セキュリティ保護装置のＩＰアドレスもしくはホスト名等の情報が格納されている。

【００５７】セキュリティ保護装置１３０は、他に、図示されていないプロセッサ５１０により実行されるプログラムを格納するためのメモリや、通信されるメッセージをキャッシングするためのキャッシュメモリ等を有する。

【００５８】図６は、ＮＡＳサーバ１２０の設定処理を示すフローチャートである。この処理は、ＰＣ１１０からＮＡＳサーバ１２０の利用に先立って、あるいは、必要に応じて適宜実施される。

【００５９】ＮＡＳサーバ１２０の設定では、まず、ＬＵの設定が行われる（ステップ６００）。

【００６０】続いて、利用可能なファイルシステムの存在が判別される。ＮＡＳサーバ１２０は、ＬＵに保持されている利用可能なファイルシステムの有無を、ＬＵ内の１ブロックに記述されているスーパーブロックのマジックナンバを参照して判定する。利用可能なファイルシステムが存在しない場合には、ステップ６０４において、ファイルシステムが構築される（ステップ６０２）。

【００６１】ファイルシステムが存在すれば（あるいは、構築された後）、そのファイルシステムが当該ＮＡＳサーバ１２０にマウントされているか判別する。この判別は、ＦＳ管理部２２３により記録されたマウント済みリストを参照して行われる。ファイルシステムが、マウントされていない場合は、ステップ６０８において、ファイルシステムのマウント処理が実施される（ステップ６０６）。

【００６２】さらに、マウントされたファイルシステムがエキスポート済みか否か判別される。この判別は、ネットワークＦＳ処理部２２２のエキスポート管理表に保持された情報の有無に基づいて行われる。ファイルシステムがエキスポートされていない場合は、ステップ６１２でファイルシステムのエキスポートが実施される（ステップ６１０）。

【００６３】図７は、ステップ６００において実施されるＬＵの設定処理の流れを示すフローチャートである。この処理により、ローカル及びリモートに存在するＬＵがＮＡＳサーバ１２０により認識される。

【００６４】ＮＡＳサーバ１２０は、管理者より、割り当てるＬＵの存在場所が、ＮＡＳサーバ１２０内のＬＵであるか、データセンタ２０内のＬＵであるかの選択を受け付ける（ステップ７００）。

【００６５】管理者によりＮＡＳサーバ１２０内のＬＵが選択された場合、ＮＡＳサーバ１２０は、記憶装置２１５の全ＬＵＮにＳＣＳＩのInquiryコマンドを発行してＬＵを検出し、そのＬＵを識別可能な情報を表示装置（図示せず）に表示する（ステップ７０２）。

【００６６】続いて、ＮＡＳサーバ１２０は、ブロックデバイスプロトコル処理部２２４により計算機システム１０とデータセンタ２０内で一意に決定されるディスク識別子を登録して、ＬＵの設定処理を終了する（ステップ７０４）。

【００６７】ステップ７００において選択されたＬＵが、データセンタ２０内に存在する場合、ＮＡＳサーバ１２０は、管理者より、リモートサイトにあるＬＵの位置情報を受け付ける。ＬＵの位置情報としては、記憶装置２５０のＩＰアドレスまたはホスト名、ｉＳＣＳＩで用いられＬＵを一意に決定するiSCSI名が用いられる。ここで、ディスク識別子とiSCSI名は、共に基本的にはＬＵを示すが、ディスク識別子にはデバイスへの接続経路となるＩ／Ｆ２１２の情報が含まれる。このため、ディスク識別子は、複数のＩ／Ｆが存在したとしても、一意なＬＵを決定することができる（ステップ７０８）。

【００６８】続いて、入力された位置情報を用い、記憶装置２５０のＬＵへの接続が試みられ、接続の可否が判別される（ステップ７１０）。接続に成功した場合、ステップ７０４の処理に移る。一方、接続に失敗した場合、ステップ７１２において、記憶装置２５０のＬＵへの通信路を確立させた後、ステップ７０４の処理に移る（ステップ７１２）。

【００６９】図８は、ステップ７１２において実施される、外部にある記憶装置２５０への通信路の確立処理を示すフローチャートである。この処理により、記憶装置２５０への通信路の確保がされる。

【００７０】まず、ＮＡＳサーバ１２０は、管理者より、データセンタ２０のセキュリティ保護装置２３０に関する認証情報の入力を受ける。そして、入力された情報に基づき、先に述べたセキュリティ保護装置管理表が

作成される（ステップ８００）。

【００７１】続いて、ＮＡＳサーバ１２０は、接続パス管理表の該当するパスのエントリに登録された情報に基づいてセキュリティ保護装置の数を取得し、セキュリティ保護装置の段数を変数“Ｓ”に設定する（ステップ８０２）。

【００７２】ＮＡＳサーバ１２０は、セキュリティ保護装置１３０へ接続する。このとき、セキュリティ保護装置１３０の安全性を高めるために認証して接続を行ってもよい（ステップ８０４）。

【００７３】ＮＡＳサーバ１２０は、データセンタ２０に到達する経路に存在する複数のセキュリティ保護装置２３０の一つに広域網経由でＴＣＰ/ＩＰを用いて接続する（ステップ８０６）。この後、セキュリティ保護装置１３０にデータセンタ側のセキュリティ保護装置２３０との接続に必要な認証情報として、セキュリティ保護装置管理表に登録されている認証情報が渡される。ＮＡＳサーバ１２０は、この認証情報による認証の可否を判定する（ステップ８０７）。

【００７４】ステップ８０７において、認証に成功すると、ＮＡＳサーバ１２０は、変数Ｓの値を１減算する（ステップ８０８）。そして、Ｓが０になったか否か、すなわち、すべてのセキュリティ保護装置について認証が完了したか判別する（ステップ８１０）。すべてのセキュリティ保護装置について認証が完了すると、ＮＡＳサーバ１２０は、セキュリティ保護装置１３０と２３０との間で通信路を確立し、目的のＬＵが含まれる記憶装置２５０への接続を行う（ステップ８１２）。

【００７５】ステップ８１０において、Ｓ＞０、すなわち認証が完了していないセキュリティ保護装置がある場合、処理はステップ８０６に戻り、次のセキュリティ保護装置への認証が行われる。

【００７６】ステップ８０７において、セキュリティ保護装置の認証に失敗した場合、ＮＡＳサーバ１２０は、認証の済んだ全てのセキュリティ保護装置との間の論理的な通信路を切断し、設定処理を終了する（ステップ８１４）。

【００７７】図９は、ステップ６０８で実施されるファイルシステムの構築処理の流れを示すフローチャートである。この処理により、認識されたＬＵ上の記憶領域に、ファイルシステムが存在していない場合、あるいはファイルシステムを作成する場合に、ファイルシステムが構築される。

【００７８】ファイルシステムの構築処理では、ＮＡＳサーバ１２０は、ＦＳ管理部２２３によりＬＵ設定処理（ステップ６０４）で検出されたＬＵを示すディスク識別子を選択する。このとき、各記憶領域上のファイルシステムの存在が、前述のスーパーブロックを確認することにより調べられる。ファイルシステムが存在すると、ファイルシステムの名称が、そのファイルシステムが構築されているＬＵに対応して表示される（ステップ９００）。

【００７９】続いて、ＮＡＳサーバ１２０は、ステップ９００でディスク識別子が表示された画面上で、管理者より、ファイルシステムを構築するＬＵに対応したディスク識別子の選択を受け付ける（ステップ９０２）。

【００８０】次に、ＮＡＳサーバ１２０は、選択されたＬＵに対するフォーマットを行うか否かを管理者に問い合わせる（ステップ９０４）。管理者によりフォーマットが指示されなければ、ファイルシステムの構築処理は終了する。管理者により、フォーマットが指示された場合は、選択された記憶領域のフォーマットを実施する。このフォーマットにより、前述のファイルシステムを構成する要素であるスーパーブロック、ｉ－ｎｏｄｅ、そして、ブロックが、選択されたＬＵに形成される（ステップ９０６）。

【００８１】図１０は、ステップ６１２で実施されるファイルシステムのマウント処理のフローチャートである。

【００８２】マウント処理では、まず、管理者よりマウントするディスク装置２５０内ＬＵの識別子が登録される。このとき、表示装置には、例えば、ＮＡＳサーバ１２０から認識できるＬＵのディスク識別子、そのＬＵに構築されているファイルシステムの名称（ある場合）、及びＬＵのマウントポイント名（ＬＵがマウント済みの場合）が対応づけられて表示される。管理者は、表示されたディスク識別子の中から、マウントしようとするＬＵのディスク識別子を選択する（ステップ１０００）。

【００８３】続いて、ＮＡＳサーバ１２０は、選択されたＬＵ内のファイルシステムがマウント可能であるか否かを、ＦＳ部２２３がメモリ内に管理しているファイルシステムのマウント済みリストから判別する（ステップ１００２）。

【００８４】選択されたＬＵのファイルシステムがマウント可能な場合、管理者からマウントポイントの指定を受け付ける（ステップ１００４）。マウントポイントが指定されると、ステップ１０００で選択されたＬＵ内のファイルシステムが、指定されたマウントポイントでＮＡＳサーバ１２０にマウントされる（ステップ１００６）。ＮＡＳサーバ１２０は、ＬＵのファイルシステムをマウント時、ファイルシステムを利用可能にする初期状態を作るために、ファイルシステムのスーパーブロック内の情報から１番目のi-node情報（ファイルシステムの基底となるルートディレクトリ）を読み出し、メモリ内に登録して処理を終了する（ステップ１００８）。

【００８５】一方、ステップ１００２において、ファイルシステムのマウントができないと判断されると、エラーが管理者に通知され、ＮＡＳサーバの設定処理が終了する（ステップ１０１０）。

【００８６】以上は、マウント時の動作処理を示した

が、ＮＡＳサーバ１２０は、マウント済みのファイルシステムの管理を終了する際には、そのファイルシステムをアンマウントする。アンマウントでは、まず、ＦＳ部のメモリ上で管理が行われているファイルシステムのi-node情報、ブロック情報、スーパーブロックの更新分がメモリからＬＵへ書き出され、ＦＳ管理部２２３内のマウント済みリストから該当ファイルシステムのエントリが削除される。

【００８７】続いて、本実施形態におけるファイルのアクセス処理について説明する。

【００８８】各ＰＣ１１０は、ファイルをアクセスしようとするとき、ＮＡＳサーバ１２０によって公開されているＬＵを、ＬＡＮ１４０を介してマウントする。ＰＣ１１０は、ＮＯＳ１１２により提供されるファイルオペレーションを用いて、マウントされたボリューム内のファイルをアクセスする。ファイルオペレーションの代表的なものには、オープン、リード、ライト、クローズなどがある。

【００８９】特定のファイルをアクセスする際には、ファイルハンドラと呼ばれるファイルごとに一意に決定される識別子が用いられる。このファイルハンドラは、ファイルのオープン時に取得される。

【００９０】図１２は、ＮＡＳサーバ１２０で実施されるファイルアクセス処理の概略を示すフローチャートである。この処理は、ＰＣ１１０からファイルオペレーションを用いて発行された、ファイルのオープン、クローズ、リード、ライトなどの要求に応じて実施される。

【００９１】ＰＣ１１０からのファイルのアクセス要求が発生すると、ネットワークＦＳ管理部２２２は、ＦＳ管理部２２３のファイルオペレーションを利用してメタデータ管理部２２３１に対して、要求された種別のファイルオペレーションに関するアクセスの許可を求める（ステップ１２０２）。

【００９２】メタデータ管理部２２３１からファイルへのアクセス制御に関する応答があると、ネットワークＦＳ管理部２２２は、その応答に基づいてアクセスの可否を判別する（ステップ１２０６）。

【００９３】アクセスが許可された場合、ＦＳ管理部２２３は、ブロックデバイスプロトコル処理部２２４に指示し、ＳＣＳＩ等のブロックデバイスプロトコルを用いたＬＵへのブロック単位でのリードとライト処理を行う。記憶領域管理部２２５は、対象とされるＬＵが記憶装置２１５にあるとき、記憶装置２１５内のＬＵに対してアクセス処理を実施する。また、対象とされるＬＵがデータセンタ２０にあるとき、記憶領域管理部２２５は、データセンタ２０の該当する記憶装置２５０のＬＵにアクセスする（ステップ１２０８）。

【００９４】ステップ１２０６において、アクセスが許可されていなかった場合、ネットワークＦＳ処理部２２２は、エラーを通知して処理を終了する（ステップ１２１０）。

【００９５】図１３は、ファイルのオープン処理におけるステップ１２０２の処理を示すフローチャートである。

【００９６】ＮＡＳサーバ１２０がＰＣ１１０から特定のファイルに対するオープン要求を受け付けると、その要求は、ネットワークＦＳ処理部２２２に入力される。ネットワークＦＳ処理部２２２は、ＦＳ管理部２２３に、ＰＣ１１０からのオープン要求で指定されたファイルのオープンを求める。ＦＳ管理部２２３は、その要求をメタデータ管理部２２３１に渡す（ステップ１３００）。

【００９７】メタデータ管理部２２３１は、ファイルアクセス管理表を参照して、指定されたファイルがすでにオープンされているか判別する。具体的には、ファイルアクセス管理表の当該ファイルに関するアクティブ項目に、いずれかのＰＣにより参照されていることを示すホスト名もしくはＩＰアドレスとファイル識別子の情報がセットされているか否かが調べられる（ステップ１３０２）。

【００９８】メタデータ管理部２２３１は、指定されたファイルがオープンされていなければ、ファイルアクセス管理表に当該ファイルのエントリを作成し、i-node情報とディスク識別子を設定する。また、アクティブ項目に、オープン要求を発行したＰＣ１１０のホスト名を設定する（ステップ１３０４）。

【００９９】次に、メタデータ管理部２２３１は、ファイルアクセスに用いられるユニークな識別子を要求元のネットワークＦＳ処理部２２２に戻す（ステップ１３０６）。

【０１００】一方、ステップ１３０２において、ファイルが既にオープンされていると判定されたとき、メタデータ管理部２２３１は、ファイルアクセス管理表の該当ファイルのレコードにＰＣ１１０のホスト名とファイルの識別子を追加する（ステップ１３０８）。そして、ステップ１３０６においてファイル識別子を戻し、このファイル識別子を用いたアクセスを可能にする。

【０１０１】図１４は、ファイルのリード処理におけるステップ１２０２の処理を示すフローチャートである。

【０１０２】ＮＡＳサーバ１２０がＰＣ１１０から特定のファイルデータのリード要求を受け付けると、その要求は、ネットワークＦＳ処理部２２２に入力される。ネットワークＦＳ処理部２２２は、ＦＳ管理部２２３に、その要求を送る（ステップ１４００）。

【０１０３】ＦＳ管理部２２３は、その要求をメタデータ管理部２２３１に渡す。メタデータ管理部２２３１は、ステップ１３０２と同様にして、リードの対象となるファイルがオープンされていてアクティブな状態か否か調べる（ステップ１４０２）。

【０１０４】ファイルがオープンされている場合、ネット

に、メタデータ管理部２２３１は、ファイルアクセス管理表を参照して、ファイルを共有している他のＰＣ１１０が存在するか調べる（ステップ１４０４）。ファイルを共有しているＰＣ１１０がある場合、メタデータ管理部２２３１は、そのＰＣ１１０に対して、バッファリングしているデータの記憶装置２５０への書き戻しを指示し、ファイルデータの一貫性を保証する（ステップ１４０６）。

【０１０５】ステップ１４０２において、ファイルがオープンされていなかったとき、ステップ１４０４において、ファイルが他のＮＡＳサーバにより共有されていなかったとき、あるいは、ステップ１４０６の処理により、記憶装置にデータが書き戻された後、ファイルアクセス管理表のi-node情報から、読み出すデータの範囲を示すブロック位置情報を取得し、ネットワークＦＳ処理部２２２に返す（ステップ１４０８）。

【０１０６】以上の処理の後、ＮＡＳサーバ１２０は、ステップ１２０８の処理により、受け取ったブロック位置情報に基づいて、記憶装置からデータを読み出す。読み出されたデータとそのサイズは、記憶領域管理部２２５からネットワークＦＳ処理部２２２に返される。ＰＣ１１０は要求したリード処理の戻り値としてサイズとデータが含まれるメモリ領域を取得する。

【０１０７】図１５は、ファイルのライト処理におけるステップ１２０２の処理を示すフローチャートである。

【０１０８】ＮＡＳサーバ１２０がＰＣ１１０からファイルへのライト要求を受け付けると、その要求は、ネットワークＦＳ処理部２２２に入力される。ネットワークＦＳ処理部２２２は、ＦＳ管理部２２３にその要求を送る（ステップ１５００）。

【０１０９】続いて、ステップ１４０２～１４０６と同様に、ファイルが既にアクティブか（ステップ１５０２）、ファイルを共有するＰＣ１１０があるか調べられ（ステップ１５０４）、ファイルを共有するＰＣ１１０がある場合に、バッファリングしているデータの書き出しの指示が行われる（ステップ１５０６）。

【０１１０】以上の処理の後、メタデータ管理部２３３１は、データを書き込むための領域（ブロック）が記憶装置２１５、２５０に確保できるか調べ、確保できれば、データ書き込みのためにその領域を割り当てる。ここでのブロックの割り当ては、従来の一般的なファイルシステムにより行われるブロックの割り当てと同様にして行われる（ステップ１５０８）。

【０１１１】領域の割り当てがすむと、割り当てられた領域の位置情報としてそのブロックアドレスがメタデータ管理部２３３１からＦＳ管理部２２３に戻される（ステップ１５１０）。

【０１１２】ＮＡＳサーバ１２０は、この後、ＦＳ管理部２２３に返されたブロックアドレスに基づいて、記憶装置２５０、あるいは記憶装置２１５にデータを書き込む。データの書き込みが終了すると、書き込まれたデータのサイズが、ＦＳ管理部２２３からネットワークＦＳ処理部２２２に返され、要求元のＰＣ１１０に、戻り値としてネットワークＦＳ処理部２２２から書き込まれたデータサイズが送られる。

【０１１３】ステップ１５０８で領域の確保ができなかった場合は、ライトアクセス不可として、エラーが返され、要求元のＰＣ１１０にその旨が通知される（ステップ１５１２）。

【０１１４】図１６は、ファイルのクローズ処理におけるステップ１２０２の処理を示すフローチャートである。

【０１１５】クローズ処理では、オープン処理と同様に、要求がネットワークＦＳ処理部２２２で受け付けられ（ステップ１６００）、対象とされるファイルがオープンされているか調べられる（ステップ１６０２）。

【０１１６】ファイルがオープンされていれば、該当するファイルについての情報をファイルアクセス管理表から削除する（ステップ１６０４）。ファイルアクセス管理表から該当ファイルのエントリを削除した後、ファイルのクローズに成功したことを通知して処理を終了する（ステップ１６０６）。

【０１１７】一方、ステップ１６０２で該当するファイルがオープンされていないと判断されたときは、メタデータ管理部はエラーを通知して処理を終える（ステップ１６０８）。

【０１１８】図１８は、セキュリティ保護装置１３０、２３０間の認証動作の手順を示すフローチャートである。

【０１１９】まず、ＮＡＳサーバ１２０からセキュリティ保護装置１３０へＴＣＰ／ＩＰで接続し（ステップ１８００）、前述の認証情報を設定する（ステップ１８０１）。この時の、ＴＣＰ／ＩＰでの接続おいて、内部からもセキュリティの維持をするために内部認証部５０６でＮＡＳサーバ１２０からの認証を行ってもよい。外部にあるセキュリティ保護装置へは、認証情報に記述されているそのセキュリティ保護装置のＩＰアドレスを用いてＴＣＰ／ＩＰを用いて接続する(ステップ１８０２)。

【０１２０】続いて、接続相手側のセキュリティ保護装置２３０に認証情報を送付する。相手側セキュリティ保護装置では、外部認証部５０９により送付された認証情報と、認証情報ＤＢ５３０に保持されている認証情報と比較して認証する（ステップ１８０６）。

【０１２１】認証に成功すれば、パス接続部５０７において、外部のセキュリティ保護装置との間で、認証情報内の暗号化アルゴリズムを元に暗号化された通信路による接続を行う（ステップ１８０８）。

【０１２２】ステップ１８０６で認証に失敗した場合は、接続元装置との間の接続が断たれる（ステップ１８１０）

【０１２３】以上のような処理により、ＮＡＳサーバ１２０から自システム内のセキュリティ保護装置１３０、データセンタ２０のセキュリティ保護装置２３０、そして記憶装置２５０それぞれの間に論理的な通信路を張ることができる。また、自システム内と他システム内でＩＰアドレスの管理形態が異なる場合があるが、このような場合は、自システムと他システム内のＩＰアドレスを変換する機構、例えば、Network Address Translator（ＮＡＴ）の機能をセキュリティ保護装置内に組み込んでもよい。

【０１２４】以上説明した実施形態によれば、ＰＣからＬＡＮ経由でＮＡＳサーバにより提供される記憶装置を利用できる。ＮＡＳサーバは、自サーバ内、あるいは外部に持つことが可能で、ＰＣに対して、記憶装置の物理的な場所を隠蔽することができる。ＰＣのユーザは、ＮＡＳサーバにより提供される記憶領域を利用するに際し、データの記憶位置を意識することなく記憶装置を利用することができる。

【０１２５】上述した実施の形態では、データセンタにある記憶装置を、異なる計算機システム１０に存在する複数のＮＡＳサーバから共有した場合に、記憶装置に保持されたデータの一貫性を維持できなくなる恐れがある。以下に、複数のＮＡＳサーバから一貫性を維持した記憶装置の共有に配慮した計算機システムの一例について説明する。

【０１２６】図１９は、本発明の第２の実施形態における計算機システムの簡略なブロック図である。

【０１２７】本実施形態における計算機システムは、複数の計算機システム１０がデータセンタ５０と広域網３０を介して接続される。本実施形態では、各計算機センタ１０のＮＡＳサーバ１２０において行われる処理が一部変更される点、及び、データセンタ５０にＮＡＳサーバ管理ホスト２１０が設けられる点を除き、第１の実施形態とほぼ同様の構成を有する。

【０１２８】ＮＡＳサーバ管理ホスト２１０は、ＮＡＳサーバ１２０間でファイルを共有する際に必要な排他管理、アクセス管理等を行う。なお、ここでは、ＮＡＳサーバ管理ホスト２１０が１台の場合について説明するが、複数台のＮＡＳサーバ管理ホスト２１０を設け、記憶装置２５０により提供される記憶領域のファイルシステムを、これら複数のＮＡＳサーバ管理ホスト２１０で分散して管理してもよい。

【０１２９】図3は、ＮＡＳサーバ管理ホスト２１０の構成を示す機能ブロック図である。ＮＡＳサーバ管理ホスト２１０は、複数のＮＡＳサーバ１２０で共用されるデータセンタ２０内の記憶装置２５０に記録されたファイルに対するデータの保証を行うための共有時のアクセス制御を行う。本実施形態では、アクセス制御をＮＡＳサーバ管理ホスト２１０で行うが、ＮＡＳサーバ管理ホスト２１０は、この機能の他、排他管理等のファイルに関する制御を備えていてもよい。

【０１３０】ＮＡＳサーバ管理ホスト２１０は、ネットワークインタフェース３１０、３３０とプロセッサ３２０を有する。この他、ＮＡＳサーバ管理ホスト２１０は、メモリや入出力装置などを有するが、これらは、本発明の説明と直接関係するものではなく、図示を省略する。

【０１３１】プロセッサ３２０は、ネットワークインタフェース３１０を介して受信したＮＡＳサーバ１２０からのファイルへのアクセスを制御する。このためにプロセッサ３２０は、ネットワークプロトコル処理部３２１、ファイルシステム管理部（ＦＳ管理部）３２２、ブロックデバイスプロトコル処理部３２３、制御部３２４を有する。プロセッサ３２０の有する各部の機能は、プロセッサ３２０上でのプログラム処理により実現される。

【０１３２】ネットワークプロトコル処理部３２１は、ネットワークプロトコル処理部２２１と同様に、ＴＣＰ／ＩＰのプロトコルに従ってＮＡＳサーバ１２０からのアクセス要求の受信処理、及び、ＮＡＳサーバ１２０へのファイルデータの送信処理を行う。ネットワークプロトコル処理部３２１は、ＮＡＳサーバ１２０からのアクセス要求の受信処理では、受信した要求をＦＳ管理部３２２に渡す。

【０１３３】ＦＳ管理部３２２は、ＮＡＳサーバ１２０のＦＳ管理部２２３と同様、ＬＵ上のファイルシステム情報を読み取り、初期状態をつくるマウント処理と終了時のアンマウントの処理、ＦＳ部２２３より要求されたファイルのアクセス要求をメタデータ処理部へ転送する機能を持つ。

【０１３４】メタデータ管理部３２２１では、アクセス中のファイルに関するi-node情報を含むファイルアクセス管理表を用いてファイルのアクセス管理を行い、複数のＮＡＳサーバ１２０によりファイルが共有された時に、ＦＳ管理部２２３より転送されたアクセス要求に対するデータの一貫性を保証する。特に、ファイルのデータやi-node情報がＮＡＳサーバ１２０のＦＳ管理部２２３でバッファリングされているときには、そのデータを一度フラッシュした後で、ファイルへのアクセスを行うよう制御する。また、第１の実施形態におけるファイルシステム管理表に記載されているマウントするファイルシステムの情報にファイル共有を許可するＮＡＳサーバ１２０のホスト名もしくはＩＰアドレスを加える。このホスト名もしくはＩＰアドレスは１つもしくは複数個あってもよい。

【０１３５】複数のＮＡＳサーバ１２０間で記憶装置２５０内のＬＵ内のファイルシステムが共有される場合、ＮＡＳサーバ管理ホスト２１０のメタデータ管理部３２２１でファイルアクセス管理表が管理される。このため、本実施形態では、各ＮＡＳサーバ１２０のＦＳ

管理部２２３は、マウント済みリストの項目として、第１の実施形態において説明した情報の他、他のＮＡＳサーバとの間でＬＵの共有が生じている場合に、その共有を管理するＮＡＳサーバ管理ホスト２１０のホスト名、あるいは、ＩＰアドレスを保持する。また、ＮＡＳサーバ１２０のメタデータ管理部２２３１で利用されるファイルアクセス管理表は、メタデータ管理部３２２１においても保持、管理される。

【０１３６】制御部３２４は、ＮＡＳサーバ１２０から要求命令されるＮＡＳサーバ管理ホスト２１０の設定を行う。

【０１３７】本実施形態では、他のハードウェア構成については、第１の実施形態と同じであり、説明を省略する。

【０１３８】本実施形態におけるＮＡＳサーバの設定は、図６に示した第１の実施形態おけるものとほぼ同様に行われる。ただし、本実施形態では、ＬＵの共有が発生するため、ステップ６１４（または６１６）の処理の後に、ＮＡＳサーバ間でのＬＵ内ファイルシステムの共有の設定が行われる。

【０１３９】具体的には、データセンタ２０にあるＬＵ上のファイルシステムの共有の有無が管理者により選択される。データセンタ２０のＬＵ上のファイルシステムを共有しない場合は、設定処理は終了する。ＮＡＳサーバ１２０間でファイルシステムを共有する場合は、ＮＡＳサーバ１２０間でのファイルシステムの共有設定を行った後、設定を終了する。

【０１４０】図１１は、ＮＡＳサーバ間でＬＵ内のファイルシステムの共有を設定するための手順を示すフローチャートである。この処理により、複数のＮＡＳサーバ１２０間で共有されるＬＵの管理が、ＮＡＳサーバ管理ホスト２１０に移管される。

【０１４１】管理者は、複数のＮＡＳサーバで共有しようとするファイルシステムを格納したＬＵを管理しているＮＡＳサーバ１２０に対して、共有しようとするファイルシステムの移管に関する情報を入力する。移管に関する情報には、共有されるＬＵとファイルシステムの指定が含まれる。（ステップ１１００）。

【０１４２】ステップ１１００で指定されたＬＵが、ＮＡＳサーバ１２０内の記憶装置２１５の記憶領域内にある場合、データセンタ２０にある記憶装置２５０に選択されたＬＵの複製が作成される。ＬＵの複製作成には、いわゆるリモートコピーと呼ばれる技術を利用できる。なお、選択されたＬＵが記憶装置２５０内に形成されたＬＵであるときは、この処理は省略される（ステップ１１０２）。

【０１４３】次に、ＮＡＳサーバ１２０内のＦＳ管理部２２３、メタデータ管理部２２３１の動作を一時的に停止（凍結）させる（ステップ１１０４）。さらに、ＮＡＳサーバ１２０は、ＦＳ管理部２２３内のファイルシステムバッファにあり、変更されているファイルに関するｉ－ｎｏｄｏ情報（ファイル管理情報）を含むメタデータをＬＵ内の所定の領域に吐き出す。メタデータの吐き出し処理が終了した後、ＮＡＳサーバ１２０は、ステップ１１０２で行ったＬＵの二重化を停止する（ステップ１１０６）。

【０１４４】ＮＡＳサーバ１２０は、ファイルの管理を移管するＮＡＳサーバ管理ホスト２１０との間の通信路を確立させる。通信路を確立するための処理は、図８において説明した、ＮＡＳサーバ１２０と記憶装置２５０との間の通信路の確立処理と同様にして行われる（ステップ１１０８）。ＮＡＳサーバ管理ホスト２１０との間の通信路を確保すると、ＮＡＳサーバ１２０は、ファイルアクセス管理表の情報の内、他のＮＡＳサーバ１２０と共有するファイルに関する情報をＮＡＳサーバ管理ホスト２１０に送る（ステップ１１１０）。

【０１４５】ＮＡＳサーバ管理ホスト２１０は、受け取ったファイルアクセス管理表の情報を参照し、アクティブとなっていたファイルをオープンする（ステップ１１１２）。続いて、ＦＳ管理部３２２を起動し、ファイルシステムの運用を開始する（ステップ１１１４）。

【０１４６】ＮＡＳサーバ１２０では、メタデータ管理部２２３１が、共有ファイルに関するメタデータをＮＡＳサーバ管理ホスト２１０に移動し、管理を移管したことをＦＳ管理部２２３に通知する（ステップ１１１６）。ＦＳ管理部２２３は、メタデータ管理部２２３１からの通知を受けると、処理を活性化させる（ステップ１１１８）。

【０１４７】処理が活性化された後、ＰＣ１１０のファイルオペレーションによりファイル操作がなされると、ＦＳ管理部２２３は、ファイルの操作に関してＮＡＳサーバ管理ホスト２１０のメタデータ管理部３２２１に命令を送信し、ブロックデバイスプロトコルを用いて記憶装置２５０と通信し、ファイルのデータを転送する。このようにして以後、ＮＡＳサーバ１２０間でファイルの共有が可能となる。

【０１４８】図１７は、ＮＡＳサーバ管理ホスト２１０で管理されているファイルシステムを含むＬＵを新たなＮＡＳサーバから利用可能とするときに実施される処理のフローチャートである。

【０１４９】まず、新たに接続しようとするＮＡＳサーバ１２０とＮＡＳサーバ管理ホスト２１０との間で認証された通信路が確保される。この処理は、図８により説明した処理と同様にして行われる（ステップ１７００）。

【０１５０】通信路が確保できた後、ＮＡＳサーバ１２０は、接続しようとするファイルシステムを含むＬＵのマウントをＮＡＳサーバ管理ホスト２１０に要求する（ステップ１７０２）。

【０１５１】ＮＡＳサーバ管理ホスト２１０は、新たな

ＮＡＳサーバ１２０からマウントの要求を受けると、そのＮＡＳサーバ１２０が、マウントを要求されたＬＵのファイルに対する操作を許可されたサーバかどうか調べる。具体的には、ファイルシステム管理表のディスク識別子に対応して、共有可能なＮＡＳサーバとしてホスト名若しくはＩＰアドレスが登録されているか調べる。ファイルシステム管理表にホスト名が設定されていれば後続のファイルの操作が許され、ホスト名若しくはＩＰアドレスが設定されていなければ、公開は許可されない。後者の場合、ステップ１７０６でエラーがＮＡＳサーバ１２０に返され処理が終了する（ステップ１７０４）。

【０１５２】公開が許される場合、ＮＡＳサーバ管理ホスト２１０は、ＮＡＳサーバ１２０に接続許可の応答を返す（ステップ１７０６）。

【０１５３】ＮＡＳサーバ１２０は、接続が許可されると、ステップ１７００と同様にして、今度は、接続しようとするＬＵを有する記憶装置２５０との間で認証された通信路を確立させる（ステップ１７１０）。

【０１５４】最後に、ＮＡＳサーバ１２０は、ファイルアクセス制御をＮＡＳサーバ管理ホスト２１０のメタデータ管理部３２２１に依頼し、後続のファイル操作を可能とする（ステップ１７１４）。

【０１５５】以上の処理により、新たなＮＡＳサーバからデータセンタに存在するファイルシステムを利用することが可能となる。ＮＡＳサーバ１２０によって共有されているファイルシステムの利用を停止する際は、ＮＡＳサーバ１２０で使用中のファイルへのオペレーションが完了し、バッファリングしているデータがファイルシステムを含むＬＵへ保管された後、ファイルシステム管理表から該当ファイルシステムのエントリが削除される。そして、第１の実施形態で説明したアンマウント処理と同様の処理がＮＡＳサーバ管理ホスト２１０で行われる。

【０１５６】ＰＣ１１０からファイルオペレーションを実行する際に実施される処理について、以下に説明を行う。なお、本実施形態では、ＮＡＳサーバ間でＬＵを共有可能とするために、第１の実施形態における処理と一部異なった処理が実施される。以下、第１の実施形態におけるファイルオペレーションとの相違点を主として説明を行う。

【０１５７】本実施形態におけるファイルのアクセス処理では、ファイルシステムのi-node、スーパーブロック、ブロックの管理などのファイルシステム管理情報が何処で管理されているかによって処理が異なる。このため、図１２におけるステップ１２０２の処理が、以下のようになる。すなわち、ＮＡＳサーバ１２０は、ＰＣ１１０からアクセス要求を受けると、マウント済みリスト内に登録されたファイルシステム管理場所を参照し、アクセスの対象とされるＬＵが、ＮＡＳサーバ１２０内のメタデータ管理部３２２１と、ＮＡＳサーバ管理ホスト２１０内のメタデータ管理部３２２１のいずれで管理されているか判別する。この判別処理は、ＦＳ管理部２２３において行われる。アクセス対象のＬＵがＮＡＳサーバ１２０内のメタデータ管理部２２３１で管理されている場合は、先に説明した第１の実施形態と同様に処理が進められる。

【０１５８】ファイルアクセスの対象となるＬＵがＮＡＳサーバ管理ホスト２１０のメタデータ管理部３２２１で管理されている場合、ＦＳ管理部２２３は、ＮＡＳサーバ管理ホスト２１０のメタデータ管理部３２２１に対してアクセス要求を送り、ファイルへのアクセス許可を求める。

【０１５９】ＮＡＳサーバ管理ホスト２１０のメタデータ管理部３２２１は、ＮＡＳサーバ１２０のＦＳ管理部３２２からアクセス要求を受けると、ファイルのオープン、リード、ライト、及びクローズの各処理においてそれぞれ図１３～図１６において説明したＮＡＳサーバ１２０のメタデータ管理部２２３１と基本的に同様の処理を実施する。ただし、図１３～図１６の処理においても、複数のＮＡＳサーバによるＬＵの共有を行うために、一部の処理が異なっている。

【０１６０】具体的に、ファイルのオープン処理では、図１３のステップ１３００において、ＮＡＳサーバ管理ホスト２１０側では、ＮＡＳサーバ１２０からオープン要求を受け取ると、要求元のＮＡＳサーバに対して、該当するファイルシステムのアクセスが許可されているか判定する。この判定は、ファイルシステム管理表を参照し、アクセスを許可されたＮＡＳサーバとして、要求元ＮＡＳサーバ１２０のホスト名、あるいはＩＰアドレスが登録されているかどうかに基づいて行われる。要求元のＮＡＳサーバ１２０によるファイルシステムのアクセスが許可されている場合は、以降のオープン処理を継続し、そうでなければ、エラーとして処理を中断する。

【０１６１】ファイルデータのリード処理時、図１４におけるステップ１４０４でメタデータ管理部３２２１は、他のＮＡＳサーバ１２０との間でファイルの共有がされているかファイルアクセス管理表を参照して判別する。ファイルの共有がある場合は、第１の実施形態において説明した処理の他、ステップ１４０６で他のＮＡＳサーバに対し、バッファリング中のデータの書き出しを要求し、データの一貫性を保証する。

【０１６２】ファイルデータのリード処理時、メタデータ管理部３２２１は、図１５のステップ１５０４において、上述したファイルデータのリード時と同様にして、他のＮＡＳサーバ１２０との間でファイルの共有がされているか判別する。ファイルを共有しているＮＡＳサーバがあれば、メタデータ管理部３２２１はステップ１５０６で他のＮＡＳサーバにバッファリングしているデータの書き出しを要求する。

【０１６３】ファイルのクローズ時、他のＮＡＳサーバ

との間でファイルが共有されているときは、ステップ１６０４においてメタデータ管理部３２２１は、該当するレコードを削除することに代えて、クローズ要求元のＮＡＳサーバに関連する情報を当該レコードから削除し、レコード自体は残す。該当レコードは、ファイルを利用するＮＡＳサーバがなくなった時点で削除される。

【０１６４】なお、本実施形態では、ＮＡＳサーバ管理ホストは、データセンタに設置され、ＮＡＳサーバとは広域網を介して接続されるが、例えば、企業内計算機システムのいずれかにＮＡＳサーバ管理ホストを設置することも可能である。この場合、その企業内計算機システムのＮＡＳサーバとＮＡＳサーバ管理ホストとは、ＬＡＮを介して接続される。

【０１６５】以上説明した実施形態によれば、異なる計算機システム上のＰＣのユーザが、ＮＡＳサーバから適用される広域網上の記憶装置上のファイルシステムを通じて、単一ファイルを共有することが可能となる。

【０１６６】

【発明の効果】本発明によれば、記憶装置の利用者がデータの保管場所を意識することなく、広域網やＬＡＮを介して安全にデータを保管し、あるいはデータの共有をすることできる。

【図面の簡単な説明】

【図１】発明が適用された計算機システムの一実施形態における構成を示す簡略なブロック図である。

【図２】ＮＡＳサーバの構成を示す機能ブロック図である。

【図３】ＮＡＳサーバ管理ホストの構成を示す機能ブロック図である。

【図４】記憶装置２５０の構成を示す簡略化された機能ブロック図である。

【図５】セキュリティ保護装置の構成を示す機能ブロック図である。

【図６】ＮＡＳサーバの設定処理の流れを示すフローチャートである。

【図７】ＬＵ設定処理の流れを示すフローチャートである。

【図８】外部の記憶装置への通信路の確立処理を示すフローチャートである。

【図９】ファイルシステムの構築処理の流れを示すフローチャートである。

【図１０】ファイルシステムのマウント処理のフローチャートである。

【図１１】ＮＡＳサーバ間でのＬＵの共有処理のフローチャートである。

【図１２】ＮＡＳサーバで実施されるファイルアクセス処理の概略を示すフローチャートである。

【図１３】ファイルのオープン処理におけるステップ１２０２の処理を示すフローチャートである。

【図１４】ファイルのリード処理におけるステップ１２０２の処理を示すフローチャートである。

【図１５】ファイルのライト処理におけるステップ１２０２の処理を示すフローチャートである。

【図１６】ファイルのクローズ処理におけるステップ１２０２の処理を示すフローチャートである。

【図１７】ＮＡＳサーバ管理ホストで管理されているファイルを新たなＮＡＳサーバから利用可能とするときに実施される処理のフローチャートである。

【図１８】セキュリティ保護装置の認証動作の手順を示すフローチャートである。

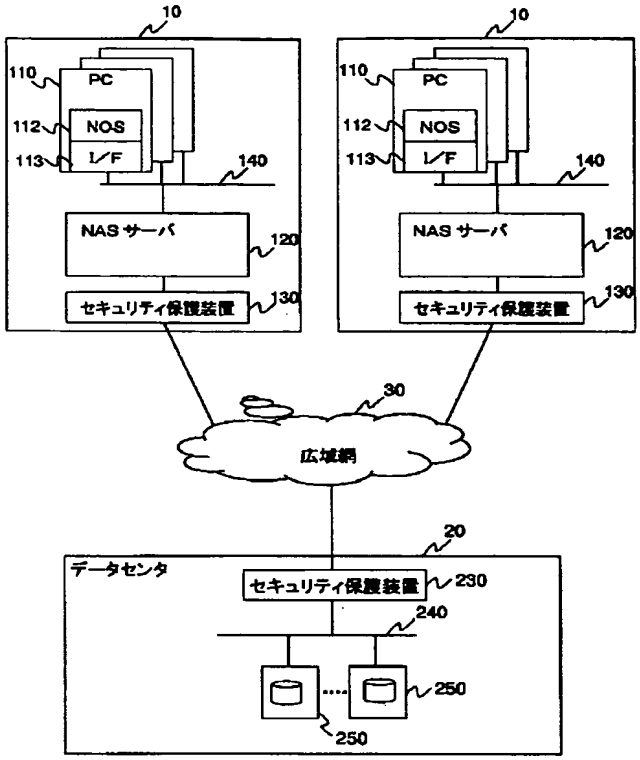
【図１９】発明が適用された計算機システムの第２の実施形態における構成を示す簡略なブロック図である。

【符号の説明】

１１０･･･パーソナルコンピュータ
１２０･･･ＮＡＳサーバ
１３０、２３０･･･セキュリティ保護装置
２１０･･･ＮＡＳサーバ管理ホスト
２５０･･･記憶装置
２２１、３２１、４１４･･･ネットワークプロトコル処理部
２２２･･･ネットワークファイルシステム処理部
２２３、３２２･･･ファイルシステム管理部
２２４、３２３、４１３･･･ブロックデバイスプロトコル処理部
２２５･･･記憶領域管理部
２２７･･･セキュリティ処理部
２２８･･･設定制御部

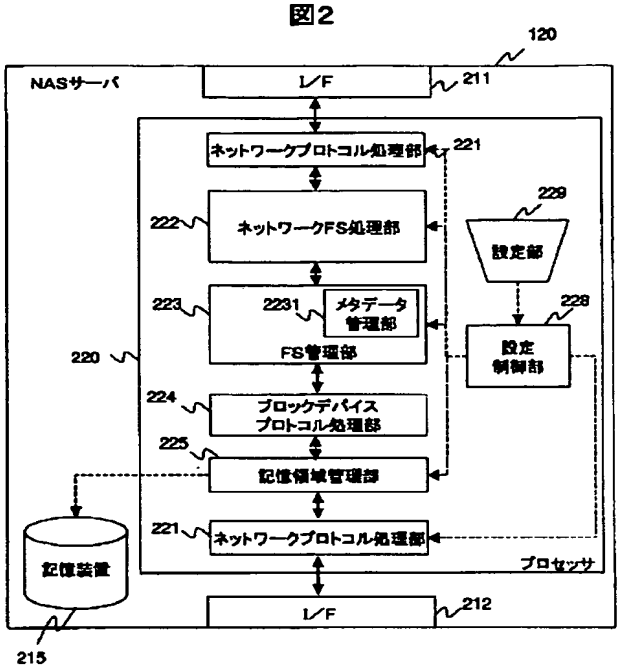
【図１】

図1



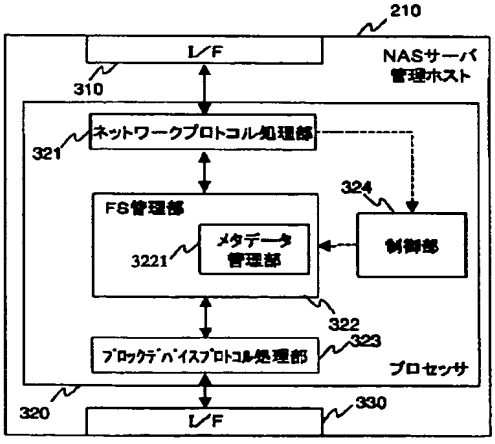
【図２】

図2



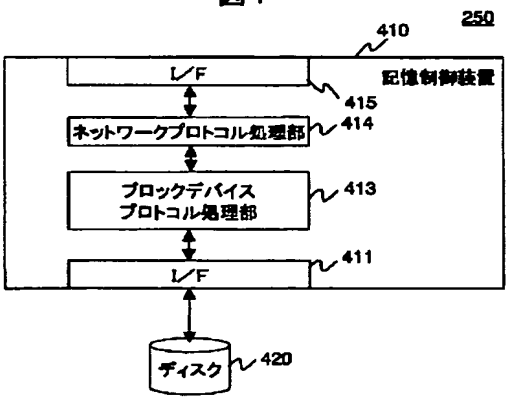
【図３】

図3



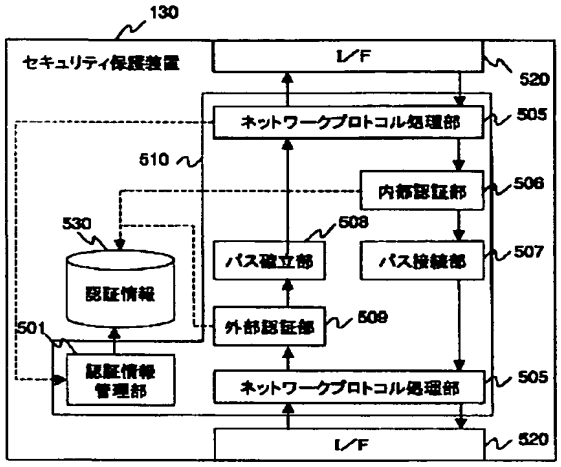
【図４】

図4



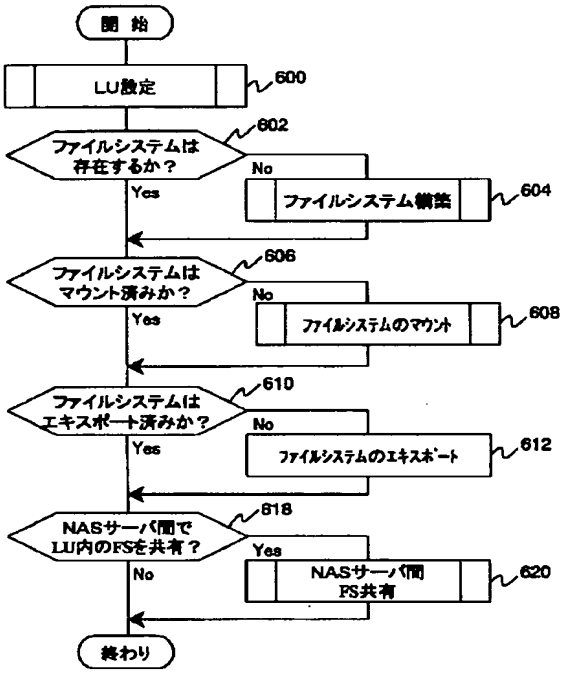
【図５】

図5



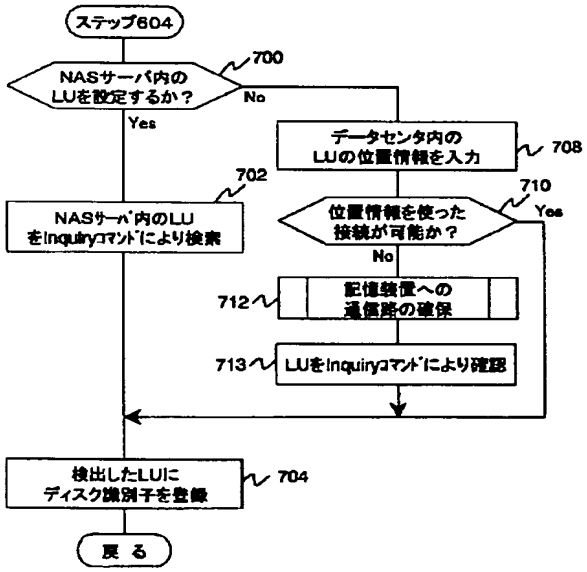
【図６】

図6



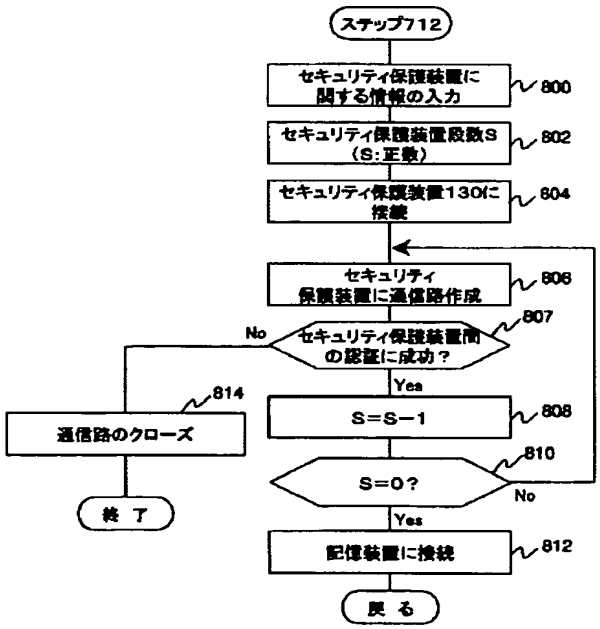
【図７】

図7



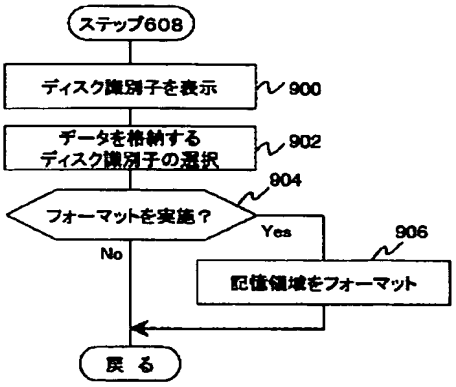
【図８】

図8



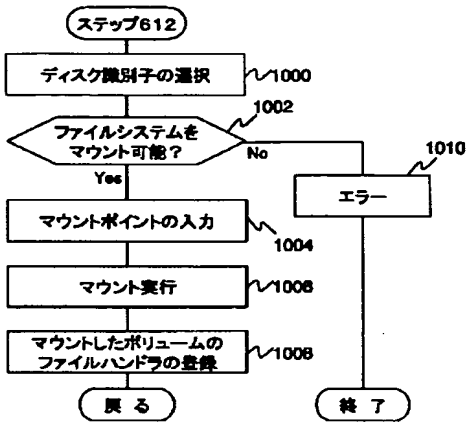
【図９】

図9



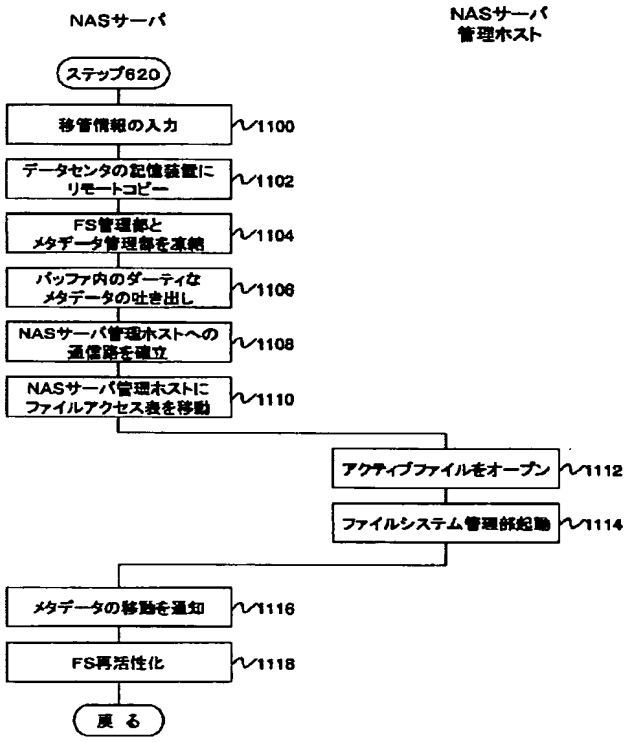
【図１０】

図10



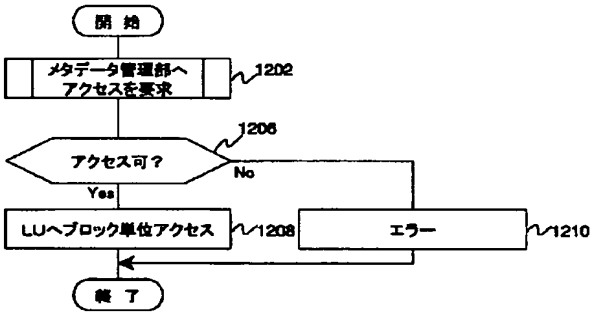
【図１１】

図11



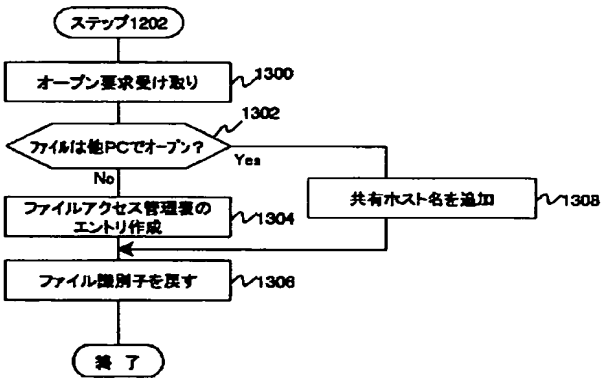
【図１２】

図12



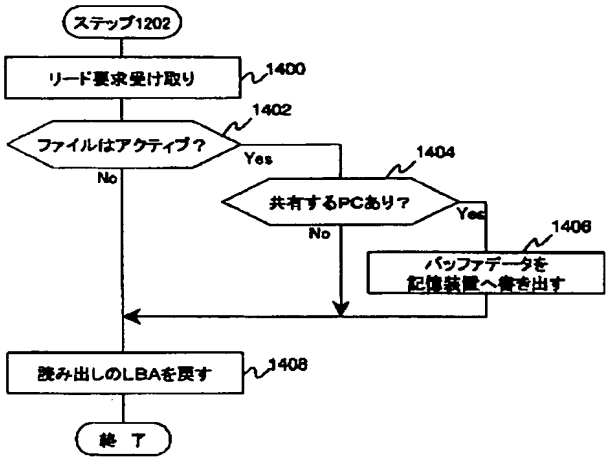
【図１３】

図13



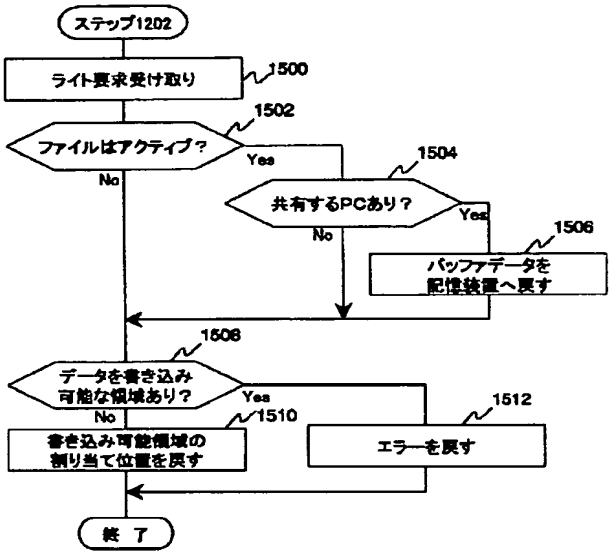
【図１４】

図14



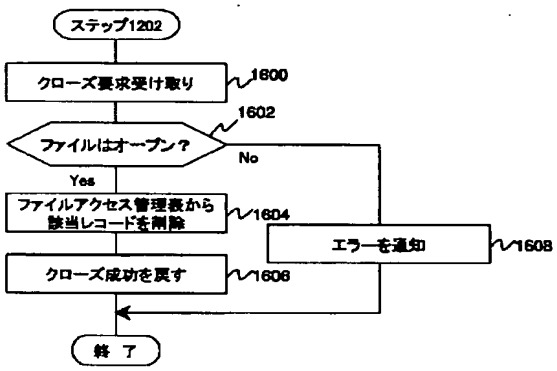
【図１５】

図15



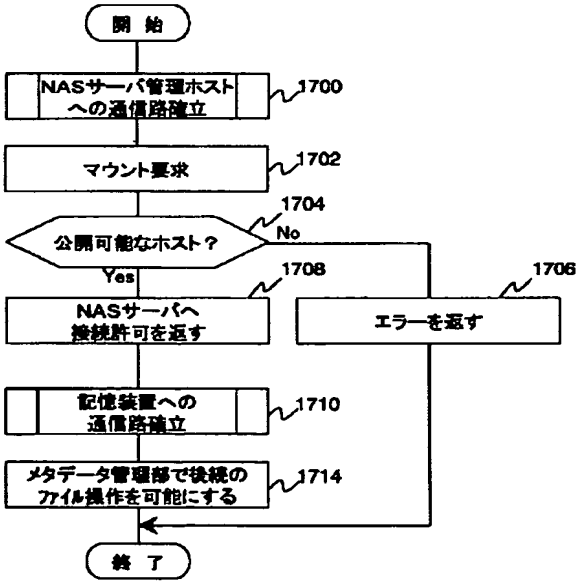
【図１６】

図16



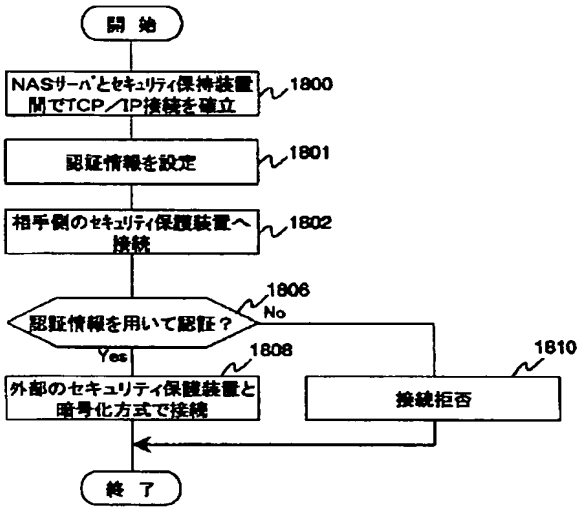
【図１７】

図17



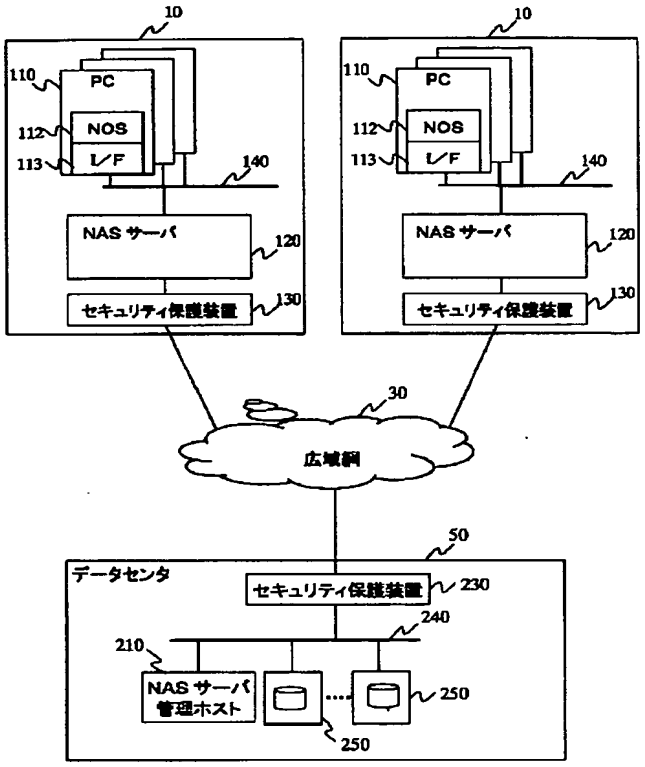
【図１８】

図18



【図１９】

図19



フロントページの続き

(72)発明者　岩村　卓成
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　▲高▼本　賢一
神奈川県小田原市中里332番地２号　株式会社日立製作所ＲＡＩＤシステム事業部内

Ｆターム(参考)　5B065 BA01 PA04 PA13
5B082 FA01 FA16
5B089 GA12 GA21 GB02 HA01 HA10
JA12 JA40 JB22 KA12 KF01